

Mr. John Mott-Smith
Director of Voting Systems
Office of the Secretary of State
1500 11th Street
Sacramento CA 95814

9 Sep 04

Subject: Addendum to Certification of the Diebold Election Systems Global Election Management Systems (GEMS) Version 1.18.19 for the VCPProgrammer, Ver.4.1.11.

Executive Summary

State certification testing was conducted 12 Sep 2004, at the California Secretary of State Election Division offices in Sacramento, CA, to certify the Diebold Election Systems VCPProgrammer, Ver. 4.1.11. The VCPProgrammer is a program which can run on a laptop or desktop computer, equipped with a compatible smart card reader/writer, to provide poll-workers with method for issuing Diebold Voter Access Cards for the AccuVote Touch Screen systems (AV-TS R6 or AV-TSx). The configuration reported here is for Early Voting with no input except an export file from GEMS 1.18.19.

VCPProgrammer supplements or replaces the hand-held Diebold Voter Card Encoders (VCE) or the table top Precinct Control Models (100 & 500). The Windows screen gives it a larger display selection and the larger memory capacity allows it to hold and to identify a voter's ballot style choices for any voter in the jurisdiction. For example, the full primary test election requires 121 ballot styles which would require 20 VCEs to create voter cards when the VCPProgrammer can handle all 121 ballot styles.

The VCPProgrammer performed as expected and produced a Voter Access Card for all variations of ballot styles in the test elections.

References:

1. [SVF0624] Freeman, *Certification of the Diebold Election Systems Global Election Management Systems (GEMS) Version 1.18.19, Key Card Tool Rev 1.0.1 , Voter Card Encoders (VCE) Rev 1.3.2, and AccuVote Touch Screen DRE (AV-TS R6), Firmware 4.3.15D*, 24 Jun 2004
2. [GEMS-U] Diebold, *GEMS 1.18 User's Guide*, Rev 9.0, 13 Feb 2004
3. [Ciber] Ciber Letter, Functional Testing of GEMS Version 1-18-19 with Central Count OS Functional Testing of GEMS Version 1-18-19 with VCPProgrammer, 7 Sep 2004
4. [VCProgUG] Diebold, *VCPProgrammer 4.1 User's Guide*, Rev 4.0, 30 Jun 2004

Introduction

In compliance with California Elections Code 19200 and 19205, Diebold Election Systems applied for certification for the following additional program:

- a. VCPProgrammer, Ver 4.1.11.

"VCPProgrammer is a PC based application that, when used with an external smart card reading device, can be used to create voter access cards for use on AccuVote-TS Ballot Station units

configured for an election. The information the application requires to create voter access cards for the election is taken from a file that has been exported from the GEMS election database. When this file has been made available to VCProgrammer, the application can be used to identify the precinct and party associated with the ballot to be copied onto a voter access card for a voter." [from ref [VCProgUG]].

VCProgrammer is also designed to interface with a Voter Registration (VR) system. In that set up, the poll worker would access the VR record and update to show the voter has come in to vote. When the poll worker updates the VR record, the VCProgrammer would get the information to select the appropriate precinct and party. The linkage with the VR system has to be tailored for the VR database and was not attempted in this certification testing. If a county were to apply to use that feature, Detailed Acceptance testing should be conducted with the actual VR system to be used in the given client jurisdiction prior to use.

A Key card produced by the Key Card Tool, using the master encryption keys set for the AV-TS terminals assigned to the local polling place, is used to configure VCProgrammer.

NASED Qualifications

Ciber, the Federal ITA testing software VCProgrammer, provided a letter [Ciber] reporting that they have completed functional testing under the Voting System Standards, 2002, and that the tests indicated that VCProgrammer satisfies the functional requirements under VSS, 2002.

Test Report Results

The same Primary test election used in prior tests was used. The test election based on San Diego 2002 Primary uses seven political parties. Three parties, American Independent, Democratic, and Republican, were defined as allowing DTS voter participation. For this test, a backup copy of the election used in the prior GEMS 1.18.19 test for the AV-TS R6 and AV-OS was loaded and reset.

An AV-TS R6 unit was setup and configured for EV operation. The VCProgrammer was used to select and produce voter access cards for declared and decline-to-state voters in Democrat, Republican, and American Independent Party. Options for Audio, Magnify, and Provisional ballots were also tested.

The cards used were also checked against a VCE set up for the same ballot styles. The cards were checked before use and after to make sure that what was created by one device could be read and the card reused.

Security Issues

The VCProgrammer, as are all the voter access card writer devices, are a necessary but serious point of vulnerability. If someone with malicious intent can gain access to the device and a supply of compatible smart cards, they could

1. Create additional cards,
2. Change a current card,
3. Copy the program/files to use on another PC,
 - a. Use the copied program/files to create voter access cards at will
 - b. Extract the encryption key being used.
4. Alter the existing program/files to interfere with other voter's access.

The VCProgrammer in EV mode is worse because (1) all the precincts/parties may be included and (2) the EV is prior to election day so there is extra time and created may be used in the election day programming (the cards are not time bound). The physical security of the

VCProgrammer PC while the program is installed on laptops is especially important because of the additional risk of theft, whether directed at the election or not.

The expectation is that the program will be installed on local office or personal laptops for all the precincts rather than having dedicated computers. As such, the computer is probably needed for other uses in the local environment and the temptation to connect and browse the internet or perform other operations will be difficult to overcome.

There is no access password on VCProgrammer.

Possible interventions

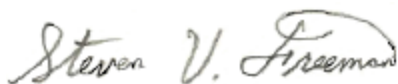
Not all of the following may be necessary, depending on local security for the polling place, but items 1, 3, and 6 should be applied

1. The master key should be changed between EV and election day.
2. Laptops/desktops in the polling places should be secured with security cables and data drives and ports (except for the port needed for the card writer) blocked or sealed while the device is being used.
3. The programs, Key Card Tool, and VCProgrammer, should be deleted from the polling place PC after they are no longer needed. This may also be an approach for overnight in early voting situations and then reinstalled the next morning. The installation is fairly quick; if the necessary files and programs are loaded on a CD-ROM, the CD can be secured in a safe until needed.
4. Use only Windows NT 2000 or XP equipped laptops.
 - a. The security management profiles should be set for high secure operations with security logging enabled.
 - b. The VCProgrammer should be setup in a special user profile that is blocked from all other applications. Diebold is investigating procedures for assigning user passwords so the login password has read only access to execute the program but does not have access to other programs.
 - c. The security logs should be recovered and checked every day for signs of unauthorized use. The logs should be retained as part of the audit trail and annotated on who/when the logs were checked.
5. No internet connection or data download/upload during use as VCProgrammer. Should an incident occur, the system should be taken out of service and checked for misuse. In case of doubt, the software should be uninstalled then reinstalled from the backup CD and the security profiles reinitialized.
6. Anti-virus and firewall programs should be installed, current, and active. The fire-walls should be set for the highest level of exclusion.

Conclusion

Review and testing of VCProgrammer showed compliance with the stated functions and intent of VCProgrammer and consistency with its use with a certified system under the California Election Code. Security is important with this component given its role in enabling voter access; local procedures will need to include specific attention to the problems of using borrowed computers in polling locations.

Sincerely,



Steven V. Freeman

Attachment:

List of the test configuration component

Attachment

Test Configuration Inventory

1. Dell Power Edge 600SC, HH18021 Chassis S/N
 - a. 1.8 gigahertz, Pentium 4 processor
 - b. 1 MByte RAM
 - c. 20 GByte IDE Internal Hard Drive
 - d. PLEXTOR CD-R PX-W1210S SCSI CdRom Drive
 - e. 3.5 Diskette Drive
 - f. ARCHIVE Python 06408-XXX SCSI Sequential Tape Drive (not used)
 - g. Digi AccelePort Xem-PCI bus card
2. DigiPorts 8/EM, PC/8em DB25, S/N: (S) V 21488435. Port 1 (COM3) and 2 (COM4)
3. Hewitt Packard Laser 1200 Printer.
4. Hayes Accura Modem External V.92 for PC-US, P/N: H08-163286, S/N 1-84-H08-15328-C1-0009 (test only)
(Normal installed version is U.S. Robotics Sportster)
5. Commercial-Off-The-Shelf Software
 - a. MS Windows 2000 Server, Service Pack 4 (Build 2195) w additional patches for SP5.
 - i. Window Internet Explorer 6.00.2800.1106
 - b. Adobe Acrobat Version 6.0.0.2003051900
 - c. Nero CD/DVD Rom Burning Suite, Version 6,
 - d. WinZip 8.1, SR1
 - e.
6. Auxiliary Equipment: AccuFeeder SN 50564 (optical connect)
7. Voting Machine Unit(s)
 - a. AV-TS R6, 156996 BS 4.3.15.D
 - i. Boot Loader 1.0.2
 - ii. C/E Aug 8, 2002
 - b. AV-OS 79811-04 30791, CC Firmware Ver. 2.0.1.2
 - c. AV-OS 79811-04 30542, CC Firmware Ver. 2.0.1.2

The test was conducted in conjunction with the testing of AV-OSCC during the same period. Although the AV-OSCC components do not use the voter access cards, the setup is listed as it exercised consistent use of the data encryption keys across all elements of the Diebold GEMS based system.